

Docket No.: 60188-806

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Customer Number: 20277
Taichi NAGATA, et al.	:	Confirmation Number:
Serial No.:	:	Group Art Unit:
Filed: March 15, 2004	:	Examiner: Unknown
For:	:	
ACCESS CONTROL SYSTEM FOR NONVOLATILE MEMORY		

**CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT**

Mail Stop CPD
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

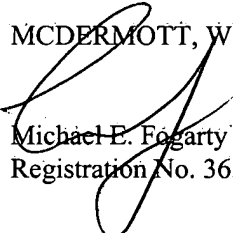
In accordance with the provisions of 35 U.S.C. 119, Applicants hereby claim the priority of:

Japanese Patent Application No. 2003-075714, filed March 19, 2003

cited in the Declaration of the present application. A certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY


Michael E. Fogarty
Registration No. 36,139

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 MEF:tlb
Facsimile: (202) 756-8087
Date: March 15, 2004

60188-806
March 15, 2004
NAGATA, et al.

日 本 国 特 許 庁
JAPAN PATENT OFFICE

McDermott, Will & Emery

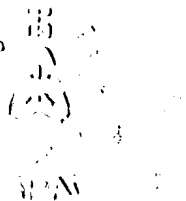
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 3 月 1 9 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 0 7 5 7 1 4
Application Number:
[ST. 10/C] : [J P 2 0 0 3 - 0 7 5 7 1 4]

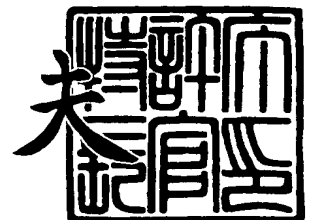
出 願 人 松下電器産業株式会社
Applicant(s):



2 0 0 4 年 2 月 3 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 4 - 3 0 0 5 5 9 1

【書類名】 特許願

【整理番号】 5037640176

【提出日】 平成15年 3月19日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 12/06

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 永田 太一

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 根本 祐輔

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100077931

【弁理士】

【氏名又は名称】 前田 弘

【選任した代理人】

【識別番号】 100094134

【弁理士】

【氏名又は名称】 小山 廣毅

【選任した代理人】

【識別番号】 100110939

【弁理士】

【氏名又は名称】 竹内 宏

【選任した代理人】

【識別番号】 100110940

【弁理士】

【氏名又は名称】 嶋田 高久

【選任した代理人】

【識別番号】 100113262

【弁理士】

【氏名又は名称】 竹内 祐二

【選任した代理人】

【識別番号】 100115059

【弁理士】

【氏名又は名称】 今江 克実

【選任した代理人】

【識別番号】 100115691

【弁理士】

【氏名又は名称】 藤田 篤史

【選任した代理人】

【識別番号】 100117581

【弁理士】

【氏名又は名称】 二宮 克也

【選任した代理人】

【識別番号】 100117710

【弁理士】

【氏名又は名称】 原田 智雄

【選任した代理人】

【識別番号】 100121500

【弁理士】

【氏名又は名称】 後藤 高志

【選任した代理人】

【識別番号】 100121728

【弁理士】

【氏名又は名称】 井関 勝守

【手数料の表示】

【予納台帳番号】 014409

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0217869

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 不揮発性メモリのアクセス制御システム

【特許請求の範囲】

【請求項 1】 不揮発性メモリと、

システム初期化のためのプログラムを格納したブート R O M と、

前記不揮発性メモリへのコマンドを発行するための C P U と、

前記 C P U からコマンドを受け取って前記不揮発性メモリへのアクセスを制御するためのアクセス制御回路とを備え、

前記 C P U は、システムの電源起動ごとに、前記ブート R O M に格納したシステム初期化のためのプログラムを実行することにより前記不揮発性メモリ上に書き換え禁止領域を、当該書き換え禁止領域上に書き込み済みフラグをそれぞれ 1 回だけ設定するように動作し、

前記アクセス制御回路は、前記書き込み済みフラグの状態を確認するまでは前記不揮発性メモリの如何なる書き込みも認めず、前記書き込み済みフラグの状態を確認した後は、前記書き込み済みフラグが書き換え禁止を示さなければ前記書き換え禁止領域への書き込みを何度でも許可するが、前記書き込み済みフラグに書き換え禁止を設定した後は前記書き換え禁止領域への書き込みを一切認めないことを特徴とする不揮発性メモリのアクセス制御システム。

【請求項 2】 請求項 1 記載のアクセス制御システムにおいて、

前記アクセス制御回路は、前記 C P U から受け取ったコマンドを解析するためのコマンド解析部を有し、

前記コマンド解析部は、前記 C P U から受け取ったコマンドが前記不揮発性メモリの書き込み又は消去を示し、その書き込み先又は消去先が前記不揮発性メモリの書き換え禁止領域であり、かつ前記書き込み済みフラグが書き換え禁止を示す場合には、前記 C P U から受け取ったコマンドを前記不揮発性メモリに伝達しないことを特徴とするアクセス制御システム。

【請求項 3】 請求項 2 記載のアクセス制御システムにおいて、

前記コマンド解析部は、前記不揮発性メモリの書き込み又は消去に特別なコマンド列を必要とする場合には、前記 C P U から受け取った全てのコマンドを解析

し、当該コマンド列が前記不揮発性メモリの書き込み又は消去を示し、その書き込み先又は消去先が前記不揮発性メモリの書き換え禁止領域であり、かつ前記書き込み済みフラグが書き換え禁止を示す場合には、前記CPUから受け取ったコマンド列を前記不揮発性メモリに一切伝達しないことを特徴とするアクセス制御システム。

【請求項 4】 請求項 2 記載のアクセス制御システムにおいて、

前記コマンド解析部は、前記不揮発性メモリの全消去に特別なコマンド列を必要とする場合には、前記CPUから受け取った全てのコマンドを解析し、当該コマンド列が前記不揮発性メモリの全消去を示し、かつ前記書き込み済みフラグが書き換え禁止を示す場合には、前記CPUから受け取ったコマンド列を前記不揮発性メモリに一切伝達しないことを特徴とするアクセス制御システム。

【請求項 5】 請求項 1 記載のアクセス制御システムにおいて、

前記不揮発性メモリ上に有用なデータを置かない未使用領域が設けられ、

前記アクセス制御回路は、前記CPUから受け取ったコマンドを解析するためのコマンド解析部を有し、

前記コマンド解析部は、前記CPUから受け取ったコマンドが前記不揮発性メモリの書き込み又は消去を示し、その書き込み先又は消去先が前記不揮発性メモリの書き換え禁止領域であり、かつ前記書き込み済みフラグが書き換え禁止を示す場合には、前記不揮発性メモリの未使用領域に対して書き込み又は消去を行うように制御することを特徴とするアクセス制御システム。

【請求項 6】 請求項 5 記載のアクセス制御システムにおいて、

前記コマンド解析部は、前記不揮発性メモリの書き込み又は消去に特別なコマンド列を必要とする場合には、前記CPUから受け取った全てのコマンドを解析し、当該コマンド列が前記不揮発性メモリの書き込み又は消去を示し、その書き込み先又は消去先が前記不揮発性メモリの書き換え禁止領域であり、かつ前記書き込み済みフラグが書き換え禁止を示す場合には、前記不揮発性メモリの未使用領域に対して書き込み又は消去を行うように制御することを特徴とするアクセス制御システム。

【請求項 7】 請求項 5 記載のアクセス制御システムにおいて、

前記コマンド解析部は、前記不揮発性メモリの全消去に特別なコマンド列を必要とする場合には、前記CPUから受け取った全てのコマンドを解析し、当該コマンド列が前記不揮発性メモリの全消去を示し、かつ前記書き込み済みフラグが書き換え禁止を示す場合には、前記不揮発性メモリの未使用領域に対して全消去を行うように制御することを特徴とするアクセス制御システム。

【請求項 8】 請求項 1 記載のアクセス制御システムにおいて、

前記アクセス制御回路は、前記不揮発性メモリ上の書き換え禁止領域に対する書き込み又は消去を検知し、かつ前記書き込み済みフラグが書き換え禁止を示す場合には、前記不揮発性メモリ上の書き換え禁止領域を除く領域中のデータを消去するように制御することを特徴とするアクセス制御システム。

【請求項 9】 請求項 1 記載のアクセス制御システムにおいて、

前記アクセス制御回路は、前記不揮発性メモリ上の書き換え禁止領域に対する書き込み又は消去を検知し、かつ前記書き込み済みフラグが書き換え禁止を示す場合には、前記不揮発性メモリ上の全データを前記書き込み済みフラグと同じ値に書き換えるように制御することを特徴とするアクセス制御システム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、不揮発性メモリのアクセス制御システムに関するものである。

【0 0 0 2】

【従来の技術】

ある従来技術によれば、課金情報、残金情報などを記憶するための不揮発性メモリに特定アドレスの書き込み回数制限回路を設けることで、ICカードの不正使用を防止する（特許文献 1 参照）。

【0 0 0 3】

他の従来技術によれば、不揮発性メモリ上にデータとプログラムとを混在させ得るように、特定アドレス領域のみデータの書き換えを可能とし、プログラム格納のための他のアドレス領域ではハードウェアにて書き換えを禁止する（特許文献 2 参照）。

【 0 0 0 4 】**【特許文献 1】**

特開平 8 - 3 2 9 2 0 8 号公報

【特許文献 2】

特開平 1 1 - 1 1 0 2 8 7 号公報

【 0 0 0 5 】**【発明が解決しようとする課題】**

例えば携帯電話において音楽、映画などの有料コンテンツの配信を受ける場合には、ユーザ I D 及びパスワードといった個人認証情報が必要である。また、暗号化されたコンテンツを復号するためには鍵情報が必要である。これらの情報を不揮発性メモリに格納して利用する場合には、その改竄を防止するセキュリティ対策が重要である。

【 0 0 0 6 】

ところが、上記特定アドレスの書き込み回数制限回路を不揮発性メモリに設ける従来技術では、システム作成者が改竄防止を必要とする情報の書き込みに失敗した場合に、再書き込みが不能になるおそれがある。

【 0 0 0 7 】

本発明の目的は、システム作成者が改竄防止を必要とする情報の書き込みを自由にでき、かつ当該情報の改竄を確実に防止できる不揮発性メモリのアクセス制御システムを提供することにある。

【 0 0 0 8 】**【課題を解決するための手段】**

上記目的を達成するため、本発明は、ブート R O M に格納したシステム初期化のためのプログラムに従って C P U が不揮発性メモリ上に書き換え禁止領域を設定し、かつ当該書き換え禁止領域上に設定した書き込み済みフラグに従ってアクセス制御回路が書き換え許可／禁止の制御を行うこととしたものである。

【 0 0 0 9 】

具体的に説明すると、本発明は、不揮発性メモリと、システム初期化のためのプログラムを格納したブート R O M と、不揮発性メモリへのコマンドを発行する

ためのCPUと、当該CPUからコマンドを受け取って不揮発性メモリへのアクセスを制御するためのアクセス制御回路とを備えた構成を採用し、CPUは、システムの電源起動ごとに、ブートROMに格納したシステム初期化のためのプログラムを実行することにより不揮発性メモリ上に書き換え禁止領域を、当該書き換え禁止領域上に書き込み済みフラグをそれぞれ1回だけ設定するように動作し、アクセス制御回路は、書き込み済みフラグの状態を確認するまでは不揮発性メモリの如何なる書き込みも認めず、書き込み済みフラグの状態を確認した後は、当該書き込み済みフラグが書き換え禁止を示さなければ書き換え禁止領域への書き込みを何度でも許可するが、当該書き込み済みフラグに書き換え禁止を設定した後は書き換え禁止領域への書き込みを一切認めないこととしたものである。

【0010】

【発明の実施の形態】

以下、添付図面を参照しながら本発明の実施形態を詳細に説明する。

【0011】

図1は、本発明に係る不揮発性メモリのアクセス制御システムの全体構成例を示している。図1の不揮発性メモリのアクセス制御システム1において、2はCPU、3はSRAM、4はブートROM、5はアクセス制御回路、6は不揮発性メモリ、7はシステムバスである。CPU2、SRAM3及びブートROM4は、システムバス7に接続されている。アクセス制御回路5は、不揮発性メモリ6とシステムバス7との間に介在する。SRAM3は、プログラム又はデータを格納するためのメモリである。ブートROM4は、システム初期化のためのプログラムを格納したメモリである。不揮発性メモリ6は、例えばフラッシュメモリである。CPU2は、SRAM3に格納したプログラム又はブートROM4に格納したプログラムを実行することにより、不揮発性メモリ2へのアクセスのためのコマンドを発行する。アクセス制御回路5は、CPU2からコマンドを受け取って不揮発性メモリ6へのアクセスを制御するための回路である。

【0012】

図2は、図1中の不揮発性メモリ6の内部構成を示している。不揮発性メモリ6は、例えばアドレス0000hから7FFFhまでの書き換え可能領域と、ア

ドレス 8000 h から FFFF h までの書き換え禁止領域とに分割される (h は 16 進数表記: 以下同じ)。更に、書き換え禁止領域上の例えばアドレス FFF0 h で指定される 1 バイト中に 1 ビットの書き込み済みフラグ F が設定される。以下の説明では、不揮発性メモリ 6 の初期状態では全ビットの値が「1」であるものとする。したがって、書き込み済みフラグ F の初期値も「1」である。ここでは、「F = 1」が書き換え許可を、「F = 0」が書き換え禁止をそれぞれ示すものとする。

【0013】

図 3 は、図 1 中のアクセス制御回路 5 の内部構成を示している。図 3 のアクセス制御回路 5 は、レジスタファイル 10 と、コマンド解析部 20 と、ライト／リード信号発行部 30 とを備えている。レジスタファイル 10 は、書き換え禁止領域アドレスレジスタ 11 と、書き換え禁止領域アドレスマスクレジスタ 12 と、書き換え禁止セクタアドレスレジスタ 13 と、書き込み済みフラグアドレスレジスタ 14 と、書き込み済みフラグビットレジスタ 15 と、書き込み済みフラグチェックコマンドレジスタ 16 と、レジスタステートマシン 17 とを有するものである。コマンド解析部 20 は、CPU 2 からシステムバス 7 を介して受け取ったコマンドを、レジスタファイル 10 を参照しながら解析する。ライト／リード信号発行部 30 は、コマンド解析部 20 での解析結果に従って不揮発性メモリ 6 の書き込み (ライト) / 読み出し (リード) / 消去 (イレース) のための信号を発行する。特に不揮発性メモリ 6 上の書き込み済みフラグ F を含む 1 バイトにアクセスする場合には、ライト／リード信号発行部 30 は、書き込み済みフラグアドレスレジスタ 14 と、書き込み済みフラグチェックコマンドレジスタ 16 とを参照する。

【0014】

図 1 中の CPU 2 は、システムの電源起動ごとに、ブート ROM 4 に格納したシステム初期化のためのプログラムを実行することにより不揮発性メモリ 6 上に書き換え禁止領域を、当該書き換え禁止領域上に書き込み済みフラグ F をそれぞれ 1 回だけ設定するように動作する。図 2 の例に従えば、書き換え禁止領域アドレスレジスタ 11 に 8000 h が、書き換え禁止領域アドレスマスクレジスタ 1

2 に 7 F F F h がそれぞれ設定される。また、書き込み済みフラグアドレスレジスタ 1 4 に F F F 0 h が、書き込み済みフラグビットレジスタ 1 5 に 3 h がそれぞれ設定される。

【 0 0 1 5 】

図 3 のアクセス制御回路 5 は、C P U 2 から書き込み済みフラグチェックコマンドが与えられて書き込み済みフラグ F の状態を確認するまでは不揮発性メモリ 6 の如何なる書き込みも認めず、書き込み済みフラグ F の状態を確認した後は、当該書き込み済みフラグ F が書き換え許可 (F = 1) を示す限りは書き換え禁止領域への書き込みを何度でも許可するが、当該書き込み済みフラグ F に書き換え禁止 (F = 0) を設定した後は書き換え禁止領域への書き込みを一切認めないように動作する。したがって、システム作成者が改竄防止を必要とする情報の書き込みを自由にでき、かつ当該情報の改竄を確実に防止できる。

【 0 0 1 6 】

図 3 中のコマンド解析部 2 0 は、C P U 2 から受け取ったコマンドが不揮発性メモリ 6 の書き込み又は消去を示し、その書き込み先又は消去先が不揮発性メモリ 6 の書き換え禁止領域であり、かつ書き込み済みフラグ F が書き換え禁止 (F = 0) を示す場合には、C P U 2 から受け取ったコマンドをライト／リード信号発行部 3 0 に伝達しないように動作する。

【 0 0 1 7 】

図 4 は、図 3 中のレジスタステートマシン 1 7 の動作を示している。レジスタステートマシン 1 7 は初期状態として、状態 1 にある。状態 1 において C P U 2 により書き換え禁止領域アドレスレジスタ 1 1 が設定されると、状態 2 に遷移する。設定されなければ状態 1 を保つ。状態 2 において書き換え禁止領域アドレスマスクレジスタ 1 2 が設定されると、状態 3 に遷移する。設定されなければ状態 2 を保つ。状態 3 において書き換え禁止セクタアドレスレジスタ 1 3 が設定されると、状態 4 に遷移する。設定されなければ状態 3 を保つ。状態 4 において書き込み済みフラグアドレスレジスタ 1 4 が設定されると、状態 5 に遷移する。設定されなければ状態 4 を保つ。状態 5 において書き込み済みフラグビットレジスタ 1 5 が設定されると、状態 6 に遷移する。設定されなければ状態 5 を保つ。

【0018】

状態6になって始めて、書き込み済みフラグチェックコマンドレジスタ16はシステムバス7からの書き込みを受け付ける。書き込み済みフラグチェックコマンドレジスタ16に書き込み済みフラグFの状態確認実行のためのコマンドが設定されると、書き込み済みフラグチェックコマンドレジスタ16はそれをライト／リード信号発行部30に伝え、ライト／リード信号発行部30は書き込み済みフラグアドレスレジスタ14に設定されたアドレスのデータを不揮発性メモリ6よりリードする。コマンド解析部20は、リードしたデータのうち書き込み済みフラグビットレジスタ15で示されるビットの値を書き込み済みフラグFとして保持する。

【0019】

レジスタステートマシン17を状態1から状態6へ遷移させ、かつ書き込み済みフラグチェックコマンドを発行することによりコマンド解析部20に書き込み済みフラグFを保持させる上記処理は、ブートROM4に格納したシステム初期化のためのプログラムをCPU2が実行することにより達成される。これらの処理が全て完了するまでは、システムバス7から不揮発性メモリ6への如何なる書き込み、消去をもコマンド解析部20により禁止する。

【0020】

書き込み済みフラグFをチェックした後のライト／消去の可否判断はコマンド解析部20で行う。具体的には、書き込み済みフラグFが書き込み許可（F＝1）を示すなら、コマンド解析部20は、書き換え禁止領域アドレスレジスタ11と書き換え禁止領域アドレスマスクレジスタ12とによって示される不揮発性メモリ6の書き換え禁止領域への書き込み、書き換え禁止セクタアドレスレジスタ13によって設定されるセクタの消去、不揮発性メモリ6上の全領域のイレーズのいずれをも許可する。したがって、システム作成者は、自分で不揮発性メモリ6上の書き込み済みフラグFを「0」に書き換えるまでは、改竄防止を必要とする情報の書き換え禁止領域への書き込みを自由にできる。しかし、システム作成者が不揮発性メモリ6上の書き込み済みフラグFを「0」に書き換えた後は、コマンド解析部20は、書き換え禁止領域への如何なる書き込み、消去も許可しな

い。なお、不揮発性メモリ 6 上の書き込み済みフラグ F のコピーをコマンド解析部 20 が常に保持することとすれば、書き込み済みフラグチェックコマンドの発行回数を削減できる。

【0021】

図 5 は、図 1 中の不揮発性メモリ 6 のコマンドの例を示している。この不揮発性メモリ 6 は、ライト及びイレーズにそれぞれ特別なコマンド列を必要とするフラッシュメモリである。図 5 中の ADRS は CPU 2 が発行するアドレスを、DATA は CPU 2 が発行するデータをそれぞれ表す。

【0022】

図 5 の上段に示すように、ライトコマンドにおいては、1 サイクル目にアドレス 555 h / データ AA h が、2 サイクル目にアドレス 2AA h / データ 55 h が、3 サイクル目にアドレス 555 h / データ A0 h がそれぞれ入力された場合に、4 サイクル目に入力されたアドレス WA に 4 サイクル目に入力されたデータ WD をライトするように決められている。

【0023】

図 5 の中段に示すように、セクタイレーズコマンドにおいては、1 サイクル目に 555 h / データ AA h が、2 サイクル目にアドレス 2AA h / データ 55 h が、3 サイクル目にアドレス 555 h / データ 80 h が、4 サイクル目にアドレス 555 h / データ AA h が、5 サイクル目にアドレス 2AA h / データ 55 h が、6 サイクル目にデータ 30 h がそれぞれ入力された場合に、6 サイクル目にデータ 30 h とともに入力されるアドレス SA で指定されたセクタのイレーズを行うように決められている。

【0024】

図 5 の下段に示すように、チップイレーズコマンドにおいては、5 サイクル目まではセクタイレーズコマンドと同様であり、6 サイクル目にアドレス 555 h / データ 10 h が入力された場合に、不揮発性メモリ 6 上の全領域のイレーズを行うように決められている。

【0025】

図 6 は、図 3 中のコマンド解析部 20 の動作を示している。コマンド解析部 2

0 は初期状態として、状態 1 にある。状態 1 においてシステムバス 7 よりアドレス 5 5 5 h / データ A A h が入力されると、状態 2 に遷移する。それ以外の入力がなされた場合には状態 1 を保持する。状態 2 においてアドレス 2 A A h / データ 5 5 h が入力されると、状態 3 に遷移する。それ以外の入力がなされた場合には状態 1 に遷移する。

【 0 0 2 6 】

状態 3 においてアドレス 5 5 5 h / データ A 0 h が入力されると、状態 4 . 1 に遷移する。状態 4 . 1 は、システムバス 7 より正常なライトコマンドが入力されたことを表す状態である。状態 4 . 1 においては、その次に入力されたアドレス W A が書き換え禁止領域アドレスレジスタ 1 1 及び書き換え禁止領域アドレスマスクレジスタ 1 2 により設定された不揮発性メモリ 6 の書き換え禁止領域に相当するかどうかをコマンド解析部 2 0 が判断する。禁止領域に相当する場合には、そのアドレスへのライトは行わない。禁止領域に相当しない場合にはそのアドレスへのデータ W D のライトを行う。

【 0 0 2 7 】

状態 3 においてアドレス 5 5 5 h / データ 8 0 h が入力されると、状態 4 . 2 に遷移する。それ以外の入力がなされた場合には状態 1 に遷移する。状態 4 . 2 においてアドレス 5 5 5 h / データ A A h が入力されると、状態 5 に遷移する。それ以外の入力がなされた場合には状態 1 に遷移する。状態 5 においてアドレス 2 A A h / データ 5 5 h が入力されると、状態 6 に遷移する。それ以外の入力がなされた場合には状態 1 に遷移する。

【 0 0 2 8 】

状態 6 においてアドレス 5 5 5 h / データ 1 0 h が入力されると、それはチップイレーズを表す。不揮発性メモリ 6 上の書き込み済みフラグ F が書き換え許可 (F = 1) を示す限り、コマンド解析部 2 0 は不揮発性メモリ 6 へのチップイレーズコマンドの発行を行う。しかしながら、不揮発性メモリ 6 上の書き込み済みフラグ F を「 0 」に書き換えた後には当該不揮発性メモリ 6 のチップイレーズは禁止するので、コマンド解析部 2 0 は不揮発性メモリ 6 へのイレーズコマンドの発行を行わない。

【 0 0 2 9 】

状態 6 においてデータ 3 0 h が入力されると、それはセクタイレーズを表す。よって、そのときに入力されたセクタアドレス S A が書き換え禁止セクタアドレスレジスタ 1 3 に設定されたセクタアドレスと異なる場合には、これに対応するセクタイレーズコマンドをコマンド解析部 2 0 が不揮発性メモリ 6 に発行する。書き換え禁止セクタアドレスレジスタ 1 3 に設定されたセクタアドレスと同一の場合には、そのセクタのイレーズは禁止するので、コマンド解析部 2 0 は不揮発性メモリ 6 へのコマンド発行を行わない。状態 6 においてそれ以外の入力がない場合には、状態 1 に遷移する。

【 0 0 3 0 】

コマンド解析部 2 0 では全コマンドが正常に入力され、かつ C P U 2 がライトしようとするアドレス、又は C P U 2 がイレーズしようとするセクタアドレスが禁止領域でないと判明してから、それまで溜め込んでおいた全てのコマンドを最初から順次ライト／リード信号発行部 3 0 に与える。したがって、ライト／リード信号発行部 3 0 へはアクセスの許可されたコマンドしか入力されないの、ライト／リード信号発行部 3 0 は、コマンド解析部 2 0 より入力される全てのアドレス／データをそのまま不揮発性メモリ 6 へ出力することができる。

【 0 0 3 1 】

以上のとおり、システムバス 7 より入力されたアドレス／データをアクセス制御回路 5 にて解析し、アクセスを許可した場合にのみ不揮発性メモリ 6 へのライト／イレーズを行う。

【 0 0 3 2 】

詳細に言うと、コマンド解析部 2 0 は、C P U 2 から受け取った全てのコマンドを解析し、受け取ったコマンド列が不揮発性メモリ 6 のライト又はセクタイレーズを示し、そのライト先又はイレーズ先が書き換え禁止領域であり、かつ書き込み済みフラグ F が書き換え禁止を示す場合には、C P U 2 から受け取ったコマンド列を不揮発性メモリ 6 に一切伝達しない。また、コマンド解析部 2 0 は、C P U 2 から受け取ったコマンド列が不揮発性メモリ 6 のチップイレーズを示し、かつ書き込み済みフラグ F が書き換え禁止を示す場合には、C P U 2 から受け取

ったコマンド列を不揮発性メモリ 6 に一切伝達しないのである。

【0033】

なお、図 1 中のブート ROM 4 のプログラムを差し替えることで図 2 中のレジスタファイル 10 の設定変更を実現すれば、不揮発性メモリ 6 上の書き換え禁止領域の設定をシステム毎に任意に変更できる。例えば、書き換え禁止領域アドレスレジスタ 11 に 4000 h を、書き換え禁止領域アドレスマスクレジスタ 12 に 3FFF h をそれぞれ設定すれば、アドレス 4000 h から 7FFF h までの領域を書き換え禁止領域に設定することができる。

【0034】

図 7 は、図 1 中の不揮発性メモリ 6 の他の内部構成を示している。ここでは、不揮発性メモリ 6 上に有用なデータを置かない未使用領域としてダミーセクタが設けられ、例えばアドレス 0010 h がダミーバイトと定められる。

【0035】

この場合、コマンド解析部 20 は、CPU 2 から受け取ったコマンド列が不揮発性メモリ 6 のライトを示し、そのライト先が書き換え禁止領域であり、かつ書き込み済みフラグ F が書き換え禁止を示す場合には、ダミーバイトに対して書き込みを行うように制御する。また、CPU 2 から受け取ったコマンド列が不揮発性メモリ 6 のセクタイレーズを示し、そのイレーズ先が書き換え禁止領域であり、かつ書き込み済みフラグ F が書き換え禁止を示す場合には、ダミーセクタに対して書き込みを行うようにコマンド解析部 20 が制御する。また、CPU 2 から受け取ったコマンド列が不揮発性メモリ 6 のチップイレーズを示し、かつ書き込み済みフラグ F が書き換え禁止を示す場合にも、ダミーセクタに対して書き込みを行うようにコマンド解析部 20 が制御する。

【0036】

このようにコマンド解析部 20 は、システムバス 7 より図 5 に示すアドレス／データを入力された都度、これをライト／リード信号発行部 30 に出力しながら、書き換え可能領域のライト／イレーズの場合にはライト先／イレーズ先を変更せず、書き換え禁止領域のライト／イレーズの場合にはライト先／イレーズ先を変更することでライト／イレーズのシーケンスを完了する。つまり、書き換え可

能領域中の一部を犠牲にするだけで、コマンド解析部 20 がコマンド列を一時的に溜め込んでおく図 2 の場合に比べて、不揮発性メモリ 6 のアクセス速度が向上するのである。

【0037】

最後に、書き換え禁止領域中の情報を改竄しようとした者にペナルティを与えることができる構成を図 8 及び図 9 に示す。

【0038】

図 8 は、図 3 中のコマンド解析部 20 の内部構成図である。図 8 において、21 はコマンド出力部、22 はライト／消去コマンド検出部、23 はイレーズコマンド発行部である。コマンド出力部 21 は、通常は CPU 2 からシステムバス 7 を介して受け取ったコマンドをそのままライト／リード信号発行部 30 へ供給する。ライト／消去コマンド検出部 22 は、書き換え禁止領域に対するライト／イレーズコマンドを検知し、かつ書き込み済みフラグ F が書き換え禁止 ($F=0$) を示す場合には、その旨をイレーズコマンド発行部 23 に伝える。これに応答して、イレーズコマンド発行部 23 は、図 3 中の書き換え禁止セクタアドレスレジスタ 13 に設定されたセクタアドレス以外の全てのセクタに対するイレーズコマンド発行命令をコマンド出力部 21 に与える。コマンド出力部 21 は、この命令に従って各セクタイレーズコマンドを発行する。これにより、改竄を防止しつつ、改竄を試みた者にペナルティを与えるように書き換え可能領域中の有用な情報が消去される。

【0039】

図 9 は、図 3 中のコマンド解析部 20 の他の内部構成図である。図 9 では、図 8 中のイレーズコマンド発行部 23 が書き込み済みフラグオーバーライト部 24 に置き換えられている。この書き込み済みフラグオーバーライト部 24 は、書き換え禁止領域に対するライト／イレーズコマンドを検知し、かつ書き込み済みフラグ F が書き換え禁止 ($F=0$) を示す旨をライト／消去コマンド検出部 22 から伝えられた場合には、図 3 中の書き込み済みフラグチェックコマンドレジスタ 16 に基づく状態確認実行により取得した書き込み済みフラグ F と同じ値 ($=0$) をライトデータとするように、全領域ライト命令をコマンド出力部 21 に与え

る。コマンド出力部 21 は、この命令に従って全領域ライトコマンドを発行する。これにより、改竄を試みた者にペナルティを与えるように、不揮発性メモリ 6 上の全データが書き込み済みフラグ F と同じ値 ($= 0$) に書き換えられる。しかも、書き込み済みフラグ F そのものは依然として書き換え禁止 ($F = 0$) を示すので、以後の書き込みも受け付けられない。

【0040】

なお、不揮発性メモリ 6 の初期状態で全ビットの値が「0」であるなら、「 $F = 0$ 」が書き換え許可を、「 $F = 1$ 」が書き換え禁止をそれぞれ示すものとすればよい。

【0041】

また、本発明は E E P R O M などの他の種類の不揮発性メモリにも適用可能である。

【0042】

【発明の効果】

以上説明してきたとおり、本発明によれば、ブート R O M に格納したシステム初期化のためのプログラムに従って C P U が不揮発性メモリ上に書き換え禁止領域を設定し、かつ当該書き換え禁止領域上に設定した書き込み済みフラグに従ってアクセス制御回路が書き換え許可／禁止の制御を行うこととしたので、システム作成者が改竄防止を必要とする情報の書き込みを自由にでき、かつ当該情報の改竄を確実に防止できる不揮発性メモリのアクセス制御システムを提供できる。

【図面の簡単な説明】

【図 1】

本発明に係る不揮発性メモリのアクセス制御システムの全体構成例を示すブロック図である。

【図 2】

図 1 中の不揮発性メモリの内部構成図である。

【図 3】

図 1 中のアクセス制御回路の内部構成図である。

【図 4】

図 3 中のレジスタステートマシンの動作を示す状態遷移図である。

【図 5】

図 1 中の不揮発性メモリのコマンド例を示す図である。

【図 6】

図 3 中のコマンド解析部の動作を示す状態遷移図である。

【図 7】

図 1 中の不揮発性メモリの他の内部構成図である。

【図 8】

図 3 中のコマンド解析部の内部構成図である。

【図 9】

図 3 中のコマンド解析部の他の内部構成図である。

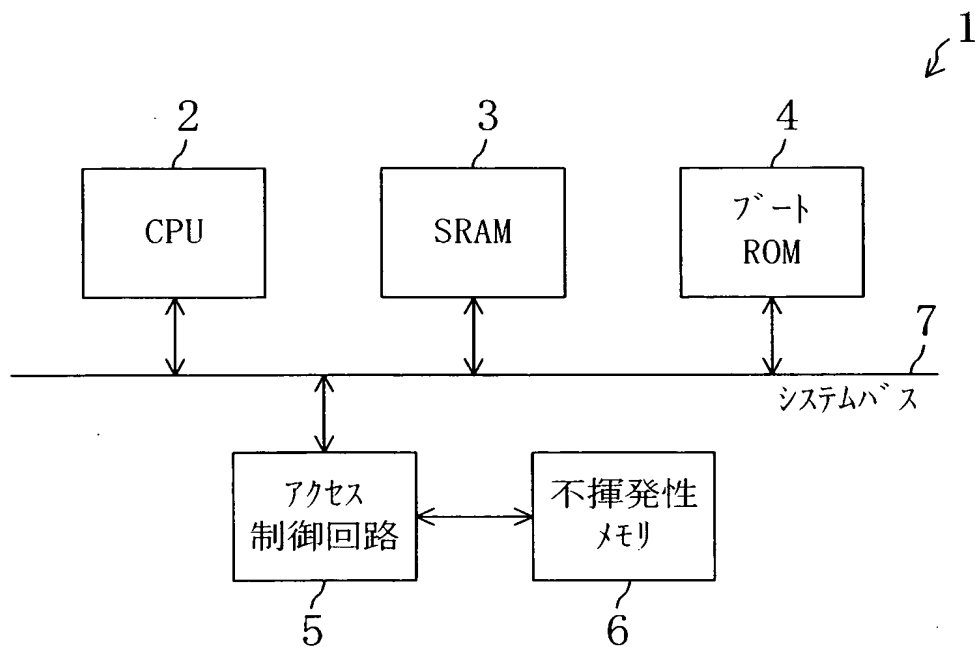
【符号の説明】

- 1 不揮発性メモリのアクセス制御システム
- 2 C P U
- 3 S R A M
- 4 ブート R O M
- 5 アクセス制御回路
- 6 不揮発性メモリ
- 7 システムバス
- 1 0 レジスタファイル
- 1 1 書き換え禁止領域アドレスレジスタ
- 1 2 書き換え禁止領域アドレスマスクレジスタ
- 1 3 書き換え禁止セクタアドレスレジスタ
- 1 4 書き込み済みフラグアドレスレジスタ
- 1 5 書き込み済みフラグビットレジスタ
- 1 6 書き込み済みフラグチェックコマンドレジスタ
- 1 7 レジスタステートマシン
- 2 0 コマンド解析部

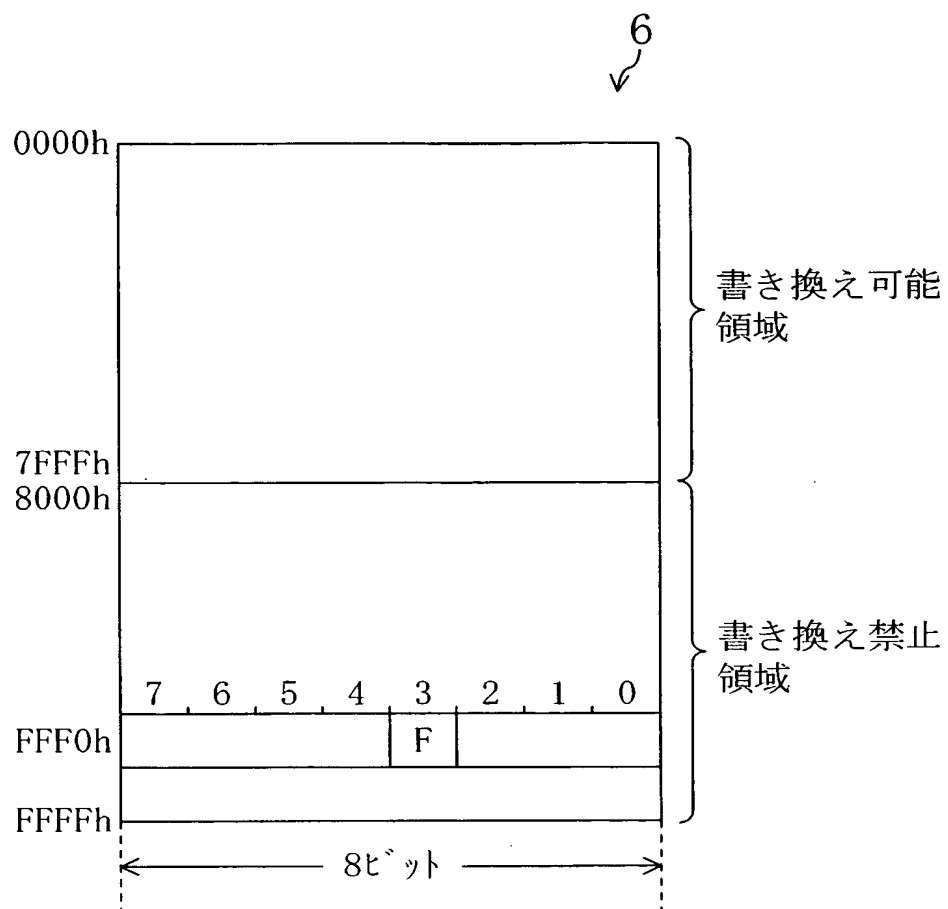
- 2 1 コマンド出力部
- 2 2 ライト／消去コマンド検出部
- 2 3 イレーズコマンド発行部
- 2 4 書き込み済みフラグオーバーライト部
- 3 0 ライト／リード信号発行部
- F 書き込み済みフラグ

【書類名】 図面

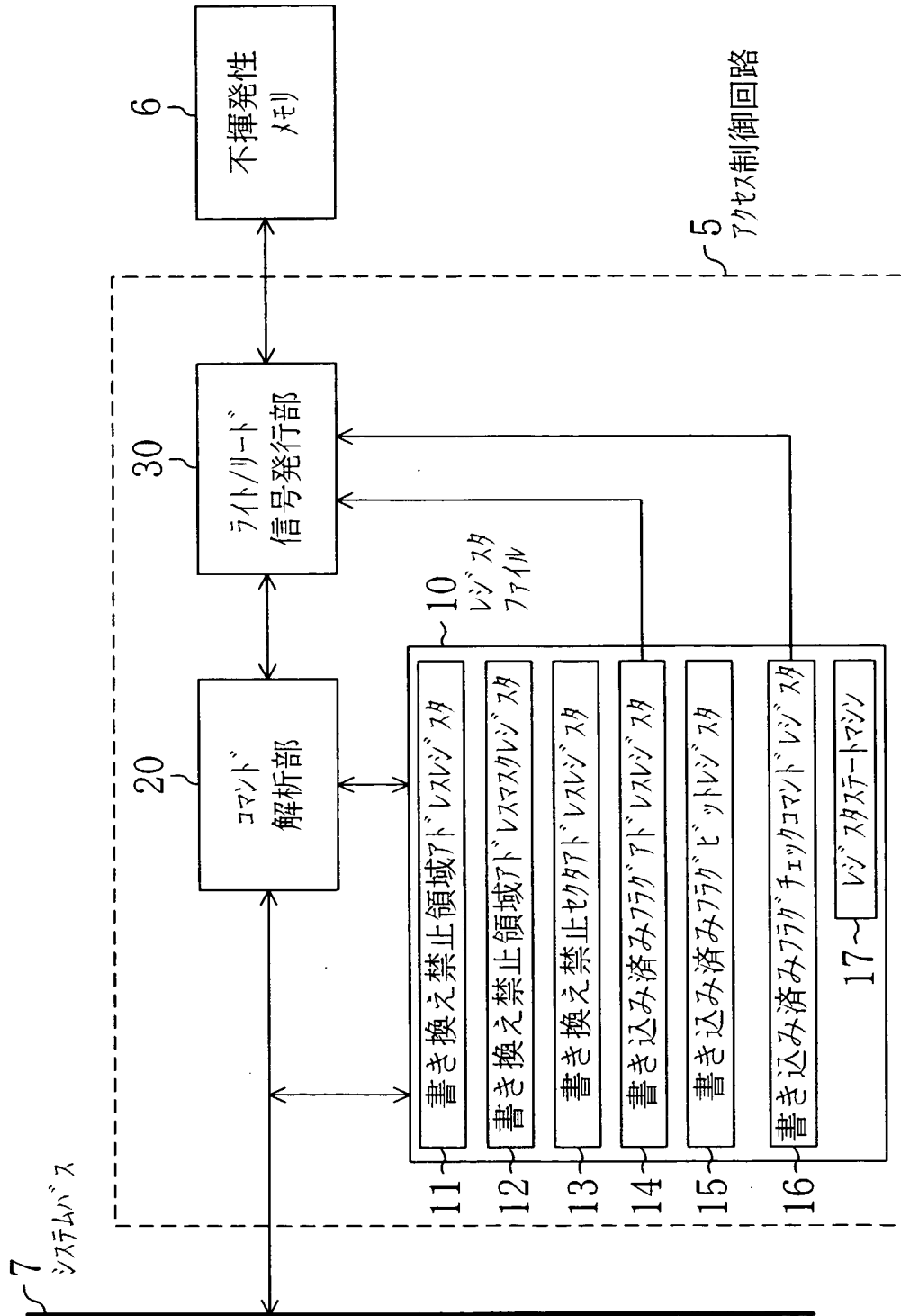
【図 1】



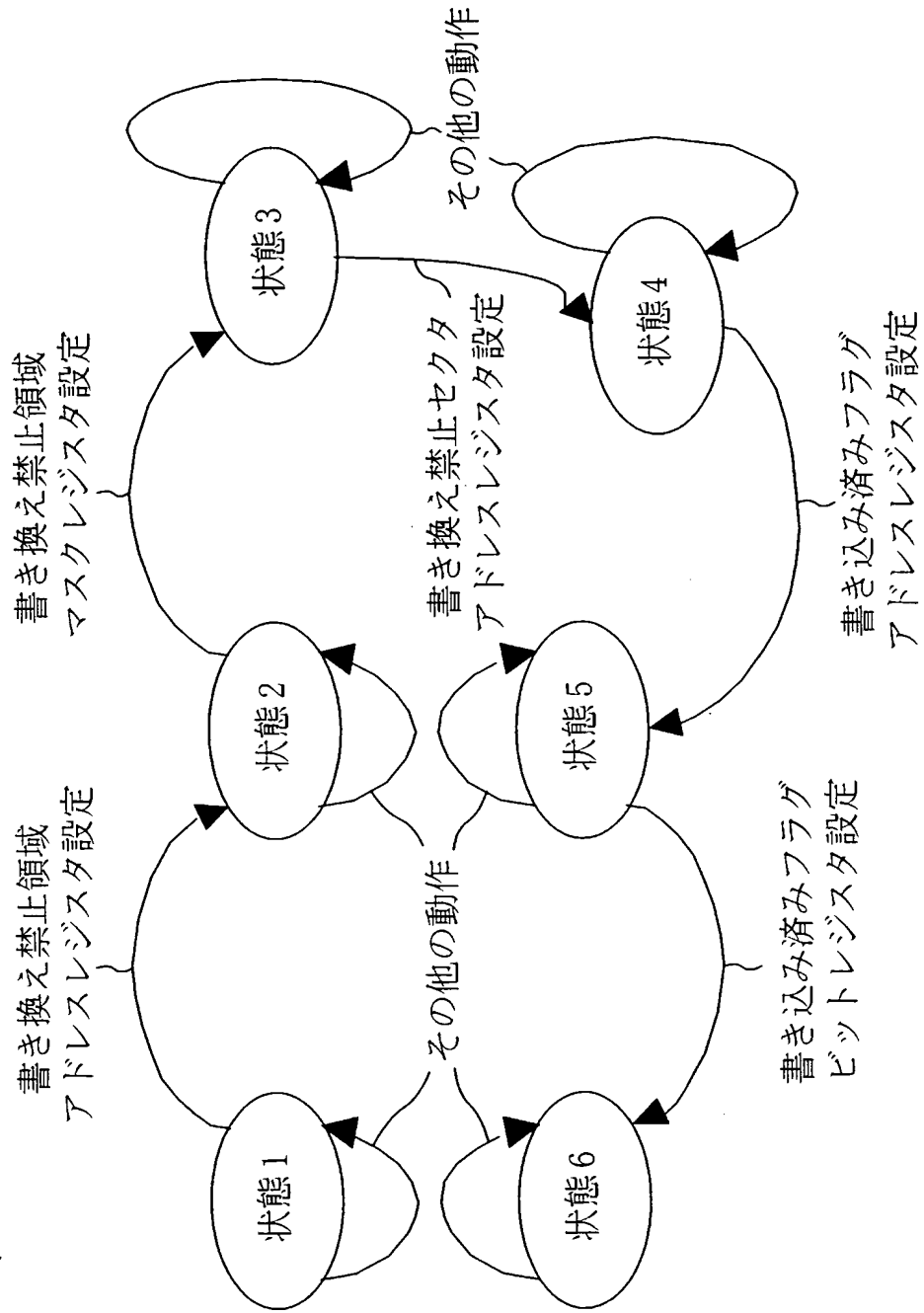
【図 2】



【図3】



【図 4】



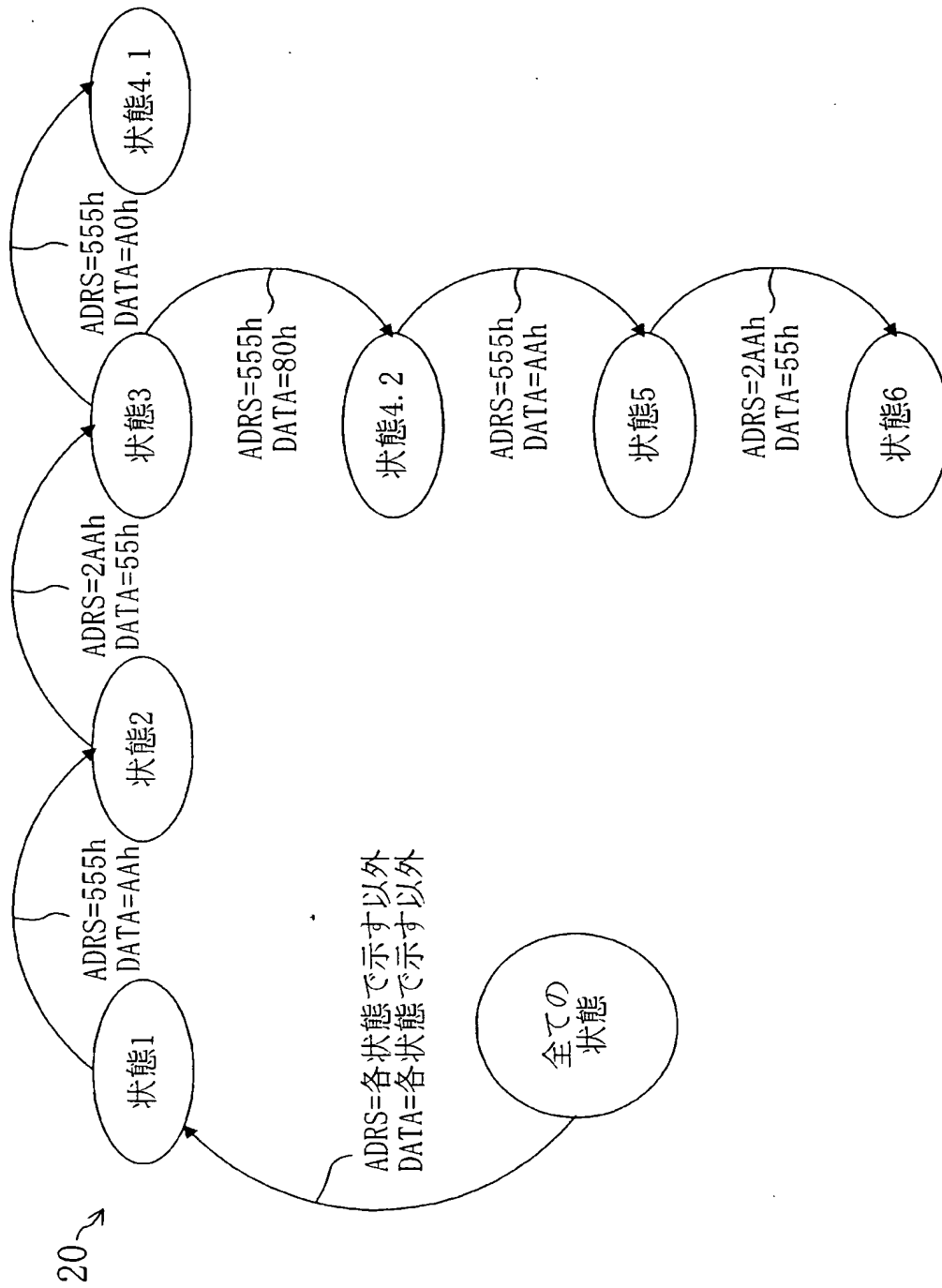
17

【図 5】

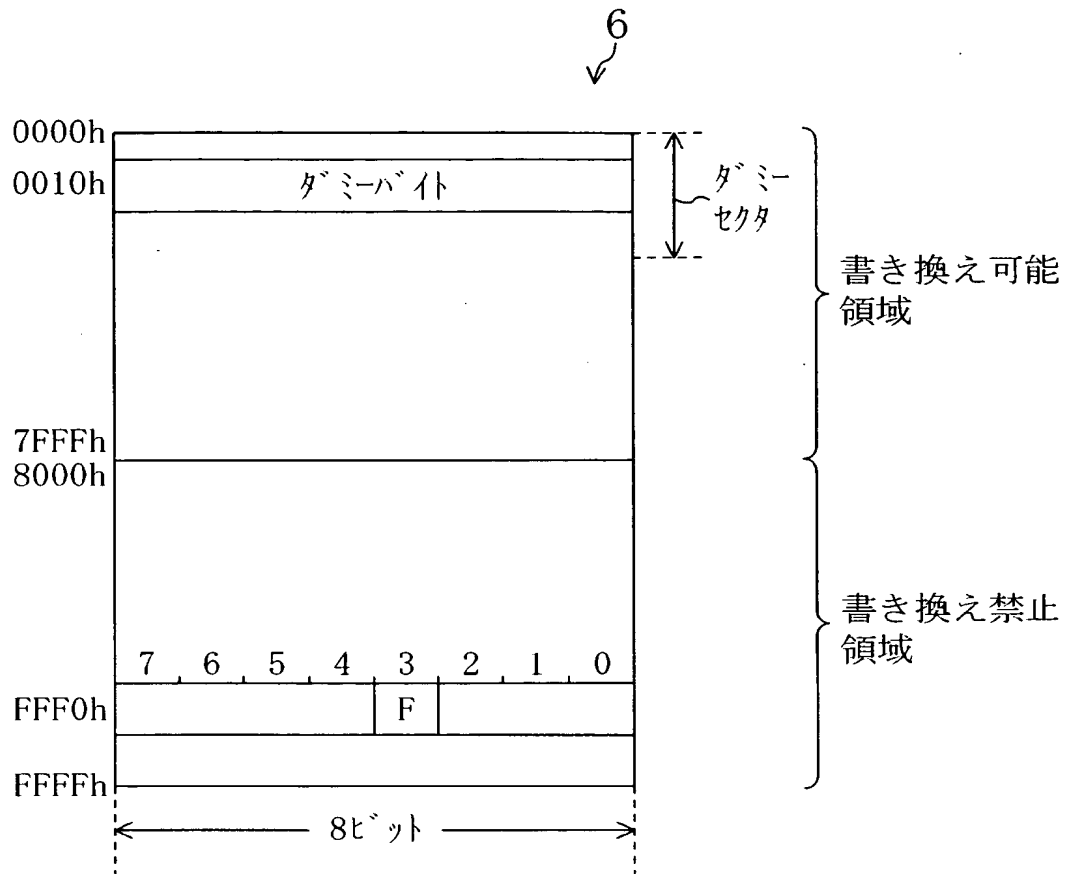
サイクル		1	2	3	4	5	6
ライト	ADRS	555h	2AAh	555h	WA	-	-
	DATA	AAh	55h	A0h	WD	-	-
セクタ イレーズ	ADRS	555h	2AAh	555h	555h	2AAh	SA
	DATA	AAh	55h	80h	AAh	55h	30h
チップ イレーズ	ADRS	555h	2AAh	555h	555h	2AAh	555h
	DATA	AAh	55h	80h	AAh	55h	10h

WA: ライトアドレス
WD: ライトデーター
SA: セクタアドレス

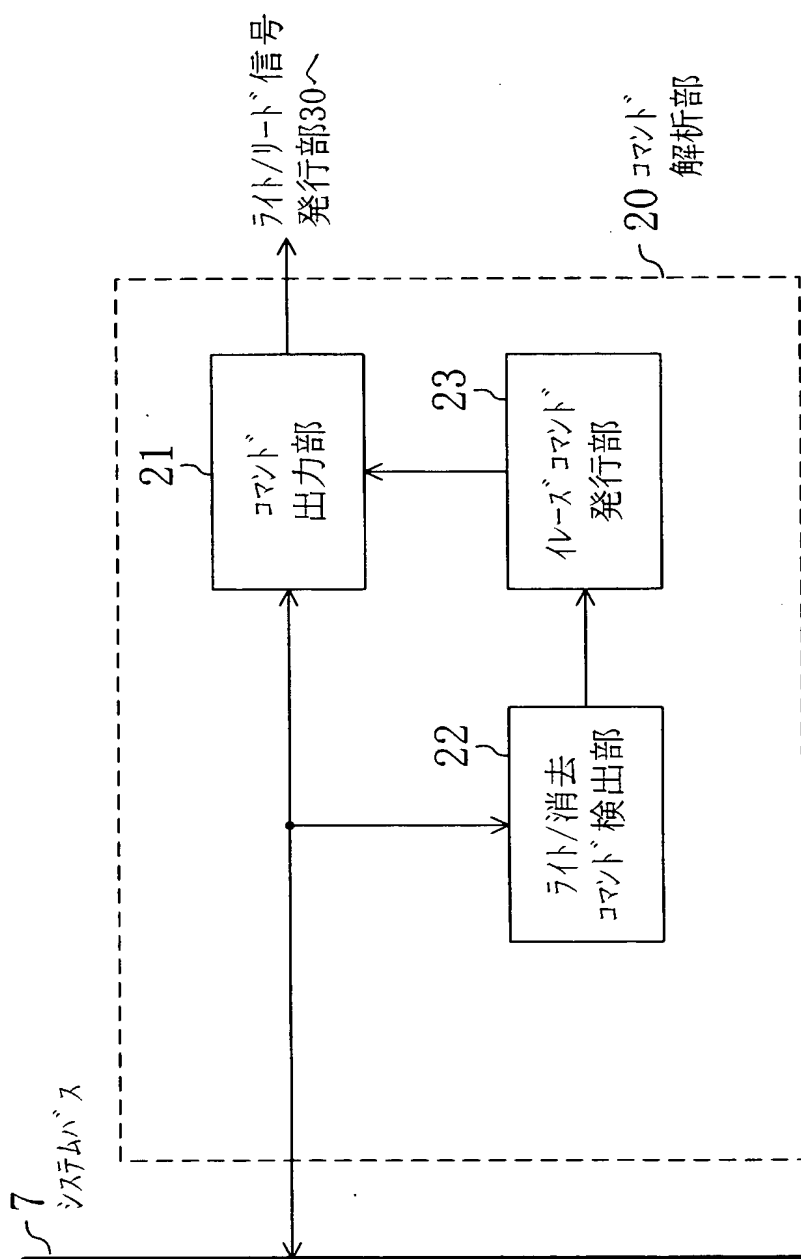
【図 6】



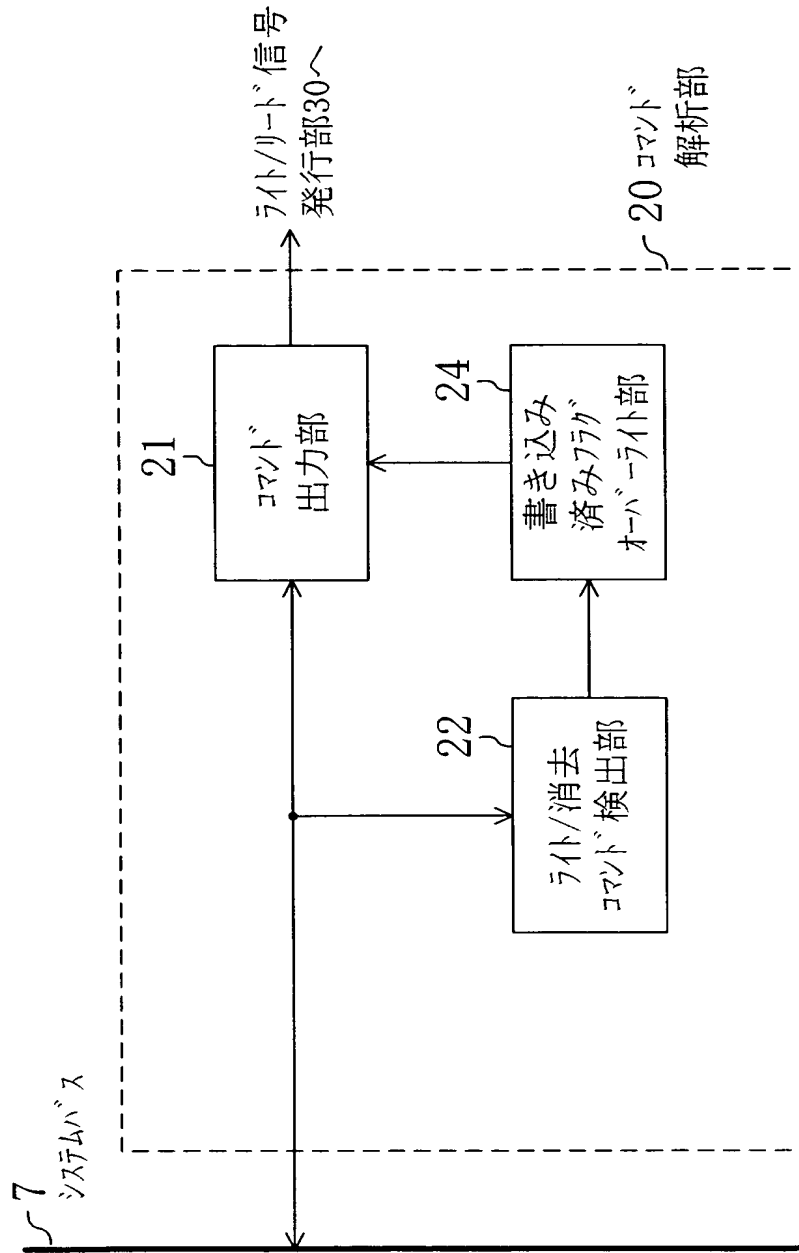
【図 7】



【図 8】



【図 9】



【書類名】 要約書

【要約】

【課題】 システム作成者が改竄防止を必要とする情報の書き込みを自由にでき、かつ当該情報の改竄を確実に防止できる不揮発性メモリのアクセス制御システムを提供する。

【解決手段】 ブートROMに格納したシステム初期化のためのプログラムに従ってCPUが不揮発性メモリ6上に書き換え禁止領域を設定し、かつ当該書き換え禁止領域上に設定した書き込み済みフラグFに従ってアクセス制御回路が書き換え許可／禁止の制御を行う。

【選択図】 図2

特願 2 0 0 3 - 0 7 5 7 1 4

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社